National Cyber Security Division
United States Computer Emergency Readiness Team (US-CERT)

Establishing and Managing a CSIRT

Reggie McKinney
Chief of Staff
US-CERT

August 8th 2006

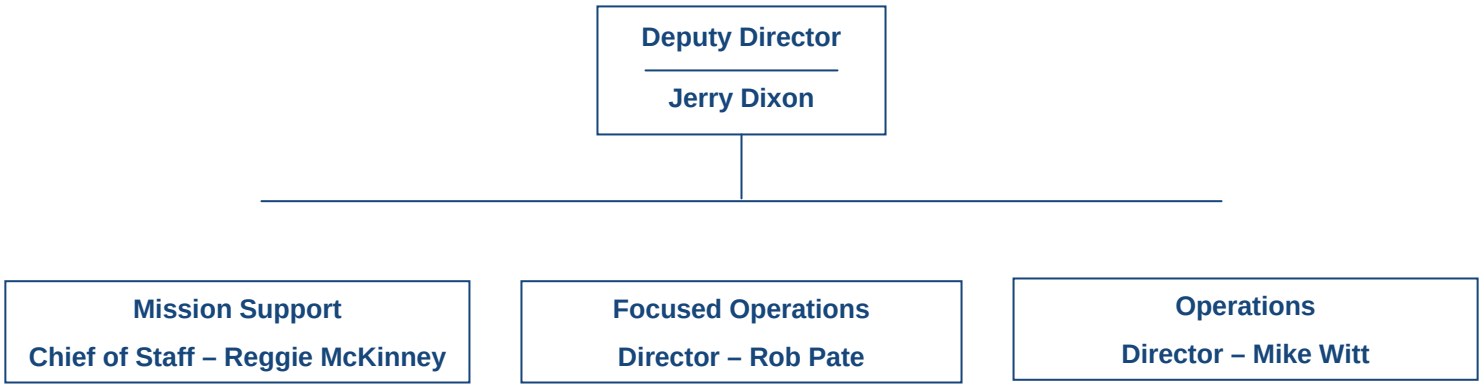
Agenda

- Introduction
- NCSD
- US-CERT Overview
- Establishing a CSIRT
- Requirements
- Operating
- Managing

NCSD/US-CERT

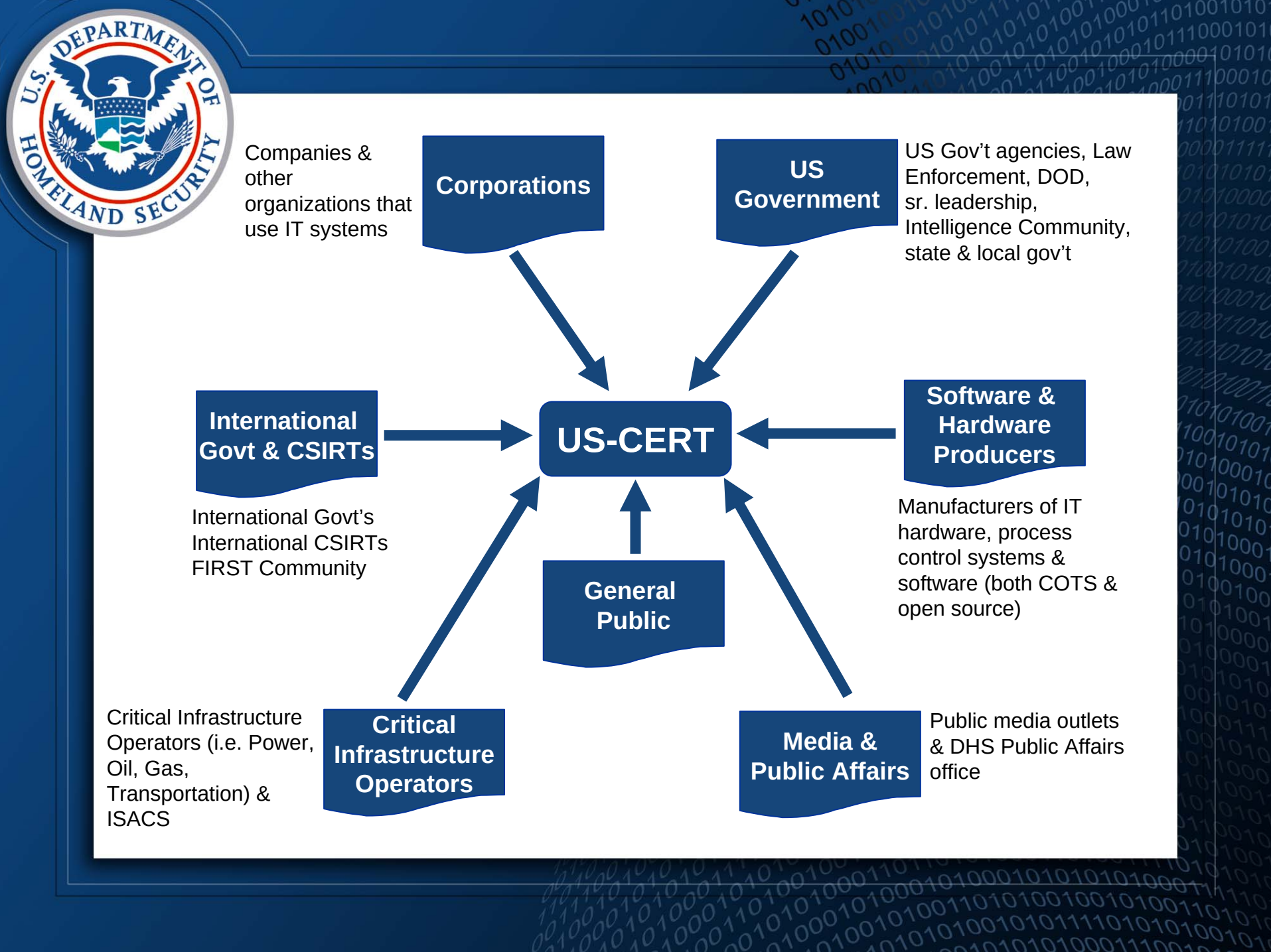
- The National Cyber Security Division is a division within the Department of Homeland Security responsible for building a national cyber security response system capable of performing analysis, issuing warnings, and coordinating response and recovery efforts.
- The United States Computer Emergency Readiness Team (US-CERT) was established in September 2003 to accelerate the process. US-CERT is the operational arm of NCSD and a partnership with the public and private sector for proving cyber analysis, event correlation and dissemination in response to cyber related activity.

US-CERT Organizational Chart



Operations

- **Incident Handling**
  - 24X7X365 triage support to federal, public, and private sector
  - Monitors cyber security events available from various sources
  - Compiles and coordinates US-CERT reports for dissemination
- **Analysis**
  - Provide fused current and predictive cyber analysis based on reporting
  - Correlates incident data from a myriad of disparate reporting sources
  - Provides on-site incident response capabilities to federal and state
- **Malware**
  - Supports forensic investigations with cursive analysis on artifacts
  - Provides on-site malware analytic and recovery support
- **Information Services**
  - Overall design and implementation of US-CERT public facing website
  - Provides operational content, design and development
  - Provides alerts, tips, bulletins in support of the National Cyber Alert System


Companies & other organizations that use IT systems
Corporations
US Government
US Gov't agencies, Law Enforcement, DOD, sr. leadership, Intelligence Community, state & local gov't
International Govt & CSIRTs
US-CERT
Software & Hardware Producers
International Govt's
International CSIRTs
FIRST Community
Manufacturers of IT hardware, process control systems & software (both COTS & open source)
General Public
Critical Infrastructure Operators (i.e. Power, Oil, Gas, Transportation) & ISACS
Critical Infrastructure Operators
Media & Public Affairs
Public media outlets & DHS Public Affairs office

Focused Operations
Initiative for Building Awareness Across the Federal Government

- US-CERT Einstein Program – An automated process for collecting, correlating, analyzing, and sharing computer security Information across the Federal civilian government.
- Allows the US-CERT to generate a cross-governmental trends analysis.
- Will help to identify configuration problems, unauthorized network traffic, network backdoors, routing anomalies, network scanning activities, and baseline network traffic patterns.
- Allows US-CERT to accomplish mission as computer incident manager for federal civilian agencies**.**

Focused Operations

- **Government Forum of Incident Response Teams (GFIRST)**
  - Community of 50+ federal agency Incident Response Teams
  - Teams work together in collaboration during on-going cyber activities for technical analysis and information sharing across the government

- **Computer Network Defense Service Provider (CNDSP) Accreditation Program**
  - Provides clear performance metrics consistency across federal civilian agencies Incident Response Teams
  - Establishes mechanism to ensure adequate funding and manpower needs to detect, report, and remediate incidents

Establishing a CSIRT

- **Motivation behind creating a Computer Security Incident Response Team (CSIRT)**
  - A general increase in the number of computer security incidents being reported
  - A general increase in the number and type of organizations being affected by computer security incidents
  - A more focused awareness by organizations on the need for security policies and practices as part of their overall risk-management strategies
  - New laws and regulations that impact how organizations are required to protect information assets
  - The realization that systems and network administrators alone cannot protect organizational systems and assets

Establishing a CSIRT

- **A few basic requirements for establishing a CSIRT**
  - What type of CSIRT will be needed?
  - What type of services should be offered?
  - How big should the CSIRT be?
  - Where should the CSIRT be located in the organization?
  - How much will it cost to implement and support a team?
  - What are the initial steps to follow to create a CSIRT?

Establishing a CSIRT

At the Start:

- Obtain management support and buy-in. Without management support it will be very difficult for the CSIRT to obtain the funding, staffing, and resources to be a success.
- Meet with key stakeholders to define the overall strategic goals of the CSIRT and to understand the needs of the constituency and services the CSIRT will offer.
- Design the CSIRT vision based on discussions about the:
  - — Constituency to be served by the CSIRT
  - — Mission, goals and objectives of the CSIRT
  - — Services provided by the CSIRT
  - — Organizational model that is most appropriate for the CSIRT and the relationship it has with the parent organization or customer base
  - — Funding to support the CSIRT start up costs and sustain its operations
  - — Resources needed by the CSIRT

Establishing a CSIRT

- **The implementation will include**:
  - Hiring and training the CSIRT staff
  - Purchasing equipment and building the CSIRT infrastructure to support the team and the needs of the constituency
  - Developing CSIRT policies and procedures to support the day-to-day operations and long-term goals and objectives
  - Developing incident reporting guidelines for the constituency, and ensuring they have access to and understand the incident reporting guidelines
  - Announcing the operational CSIRT to the community at large
  - Identifying a mechanism to evaluate the effectiveness of the CSIRT (e.g., feedback from the constituency) and improving CSIRT processes as needed

Contact

- **Technical comments or questions**
  US-CERT Security Operations Center
  Email: soc@us-cert.gov
  PGP/GPG key: 0xADC4BCED
  Fingerprint: 02FD 5294 A076 0ACE BEB1 929B 3730 09F3 ADC4 BCED
  Phone: +1 888-282-0870
- **Media inquiries**
  US-CERT Public Affairs
  Email: media@us-cert.gov
  PGP/GPG key: 0x10A97BAC
  Fingerprint: 2762 28CF AFF6 EADB 95F4 6797 857D 91C1 10A9 7BAC
  Phone: +1 202-282-8010
- **General questions or suggestions**
  US-CERT Information Request
  Email: info@us-cert.gov
  PGP/GPG key: 0x0A1E0DF7
  Fingerprint: CFE4 9D1D 6897 44B3 9B85 B25A F575 177B 0A1E 0DF7
  Phone: +1 703-235-5110
- * Information available at http://www.us-cert.gov/contact.html

Homeland Security